Journal of Pure and Applied Algebra 58 (1989) 279–287
North-Holland

EVERY FINITELY GENERATED SUBMONOID OF A FREE MONOID HAS A FINITE MALCEV'S PRESENTATION

J.C. SPEHNER
Faculté des Sciénces et Techniques, Université de Haute Alsace, 68093 Mulhouse, France

Communicated by J. Rhodes
Received 13 January 1986
Revised 1 March 1988

There exist finitely generated submonoids of a free monoid which are not finitely presented and have even not a finite cancellative presentation.

If Σ^* is the free monoid on the alphabet Σ and if $\varrho \subset \Sigma^* \times \Sigma^*$, let $m(\varrho)$ be the smallest congruence of Σ^* containing ϱ such that the monoid $\Sigma^*/m(\varrho)$ can be embedded in a group. If a monoid M is isomorphic to $\Sigma^*/m(\varrho)$, then (Σ, ϱ) is said to be a Malcev's presentation of M.

We shall prove here the following theorem: "Every finitely generated submonoid of a free monoid has a finite Malcev's presentation and such a presentation can be effectively found".

The necessary and sufficient conditions for embedding a semigroup in a group given by A.I. Malcev and a graph for determining the relators are used to prove this theorem.

1. The graph of relators of a submonoid of a free monoid

Definition 1.1. Let A^* be the free monoid on the alphabet A with identity element 1, M a submonoid of A^*, $M^+ = M \setminus \{1\}$, $C = M^+ \setminus (M^+)^2$ the generating set of $M = C^*$, α_0 a one-to-one mapping of a set Σ onto C and α the unique homomorphism of the free monoid Σ^* on the alphabet Σ onto C^*.

(i) If $z \in \Sigma$, $\omega \in \Sigma^*$ and $d, d' \in A^*$ are such that $\alpha(z) = d\alpha(\omega)d'$, $d\alpha(\omega) \neq 1$ and $\alpha(\omega)d' \neq 1$, then (d, d') is called a *Σ-pair* relative to z, (z, ω) is called the *pattern produced by* (d, d') and $(d, d')_{(z,\omega)}$ is called a *labelled Σ-pair*.

Moreover $(1,1)_{(1,1)}$ is also a labelled Σ-pair.

(ii) $\forall u \in A^+$, let $\mathrm{Fl}(u)$ [resp. $\mathrm{Fr}(u)$] be the set of left [resp. right] factors of u not in $\{u, 1\}$.

Let $\mathrm{Fl}(C) = \bigcup_{u \in C} \mathrm{Fl}(u)$, $\mathrm{Fr}(C) = \bigcup_{u \in C} \mathrm{Fr}(u)$ and $\mathrm{Fb}(C) = \mathrm{Fl}(C) \cap \mathrm{Fr}(C)$.

(iii) Let $\mathscr{G}(C)$ be the directed multigraph defined by the set $\mathrm{Fl}(C) \cup \mathrm{Fr}(C) \cup \{1\}$ of vertices and where the arcs are the labelled Σ-pairs.

The subgraph $\mathscr{L}(C)$ of $\mathscr{G}(C)$ which is the strong connected component of 1 in $\mathscr{G}(C)$ is called the *graph of relators of* C^*.

(iv) If $\sigma = ((d_0, d_1)_{(z_1,\omega_1)}, (d_1, d_2)_{(z_2,\omega_2)}, \ldots, (d_{n-1}, d_n)_{(z_n,\omega_n)})$ is a path of $\mathscr{L}(C)$ which length n is even [resp. odd], the pair

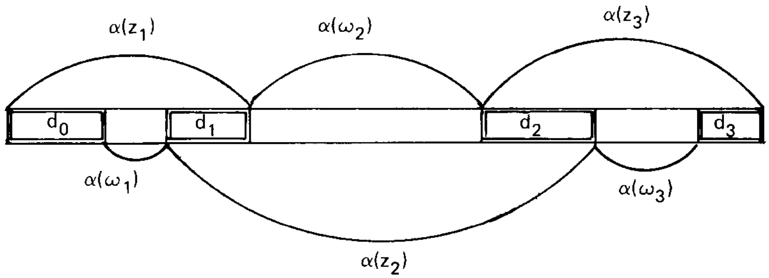

Fig. 1.

$$(u, u') = (z_1 \omega_2 z_3 \dots z_{n-1} \omega_n, \omega_1 z_2 \omega_3 \dots \omega_{n-1} z_n)$$

(resp$(u, u') = (z_1 \omega_2 z_3 \dots \omega_{n-1} z_n, \omega_1 z_2 \omega_3 \dots z_{n-1} \omega_n)$) and its inverse (u', u) are called the *patterns produced by the path* σ.

If n is even, then

$$\alpha(z_1 \omega_2 \dots z_{n-1} \omega_n) d_n = d_0 \alpha(\omega_1 z_2 \dots \omega_{n-1} z_n)$$

and if n is odd, then

$$\alpha(z_1 \omega_2 \dots \omega_{n-1} z_n) = d_0 \alpha(\omega_1 z_2 \dots z_{n-1} \omega_n) d_n.$$

Fig. 1 gives a geometric interpretation for this relation (with $n=3$).

(v) Every path $\sigma = ((d_0, d_1)_{(z_1, \omega_1)}, \dots, (d_{n-1}, d_n)_{(z_n, \omega_n)})$ such that $d_0 = d_n = 1$ is called a *unitary circuit*.

(vi) Every pair $(u, v) \in \Sigma^* \times \Sigma^*$ such that $\alpha(u) = \alpha(v)$ is called a *relator of* C^*.

Theorem 1.2. *Let C be the smallest generating set of a submonoid of the free monoid A^* on the alphabet A.*

(i) *For every unitary circuit σ of $\mathscr{L}(C)$, the patterns produced by σ are relators of C^*.*

(ii) *For every relator (u, v) of C^*, there exists a unique unitary circuit σ of $\mathscr{L}(C)$ such that (u, v) and (v, u) are the patterns produced by σ.*

This theorem is proved in [11] and in [13] (see also [6, pp. 110–115]).

Example 1.3. Let $A = \{a, b\}$, $\Sigma = \{x, y, z, u\}$, α the unique homomorphism of Σ^* into A^* such that $\alpha(x) = a$, $\alpha(y) = ab$, $\alpha(z) = ba$ and $\alpha(u) = bb$ and $C = \alpha(\Sigma)$.

The graph of relators of C^* is then given in Fig. 2.

(xz, yx) and (xux, yz) are relators of C^* respectively produced by the unitary circuits

$$((1, b)_{(y,x)}, (b, 1)_{(z,x)}) \quad \text{and} \quad ((1, b)_{(y,x)}, (b, b)_{(u,1)}, (b, 1)_{(z,x)}).$$

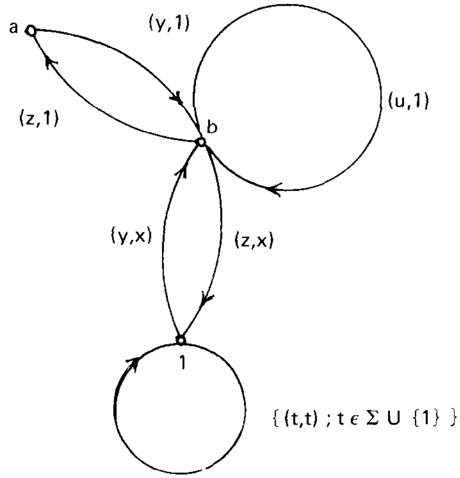

Fig. 2.

2. The finite Malcev's presentation of a finitely generated submonoid of a free monoid

Definition 2.1. A congruence τ of a monoid M is called a *Malcev's congruence* if the quotient monoid M/τ is embeddable in a group.

If $(\tau_i)_{i\in I}$ is a family of Malcev's congruences of a monoid M, then $\tau=\bigcap_{i\in I}\tau_i$ is also a Malcev's congruence since, $\forall i\in I$, M/τ_i is embeddable in a group G_i and, consequently M/τ is embeddable in the product $\prod_{i\in I}(M/\tau_i)$ which is embeddable in the group product $\prod_{i\in I}G_i$.

There exist therefore, $\forall\varrho\subset M\times M$, a smallest Malcev's congruence $m(\varrho)$ of M containing ϱ.

If Σ^* is the free monoid on the alphabet Σ and if $\varrho\subset\Sigma^*\times\Sigma^*$, (Σ,ϱ) is called a *Malcev's presentation* of every monoid isomorphic to $\Sigma^*/m(\varrho)$.

If Σ and ϱ are finite, this *presentation* is said to be *finite*.

Definition 2.2. Let $\bar{\Sigma}$ and $\bar{\bar{\Sigma}}$ be two sets in bijection with Σ and such that $\Sigma\cap\bar{\Sigma}=\Sigma\cap\bar{\bar{\Sigma}}=\bar{\Sigma}\cap\bar{\bar{\Sigma}}=\emptyset$, $z\to\bar{z}$ [resp. $z\to\bar{\bar{z}}$] a one-to-one mapping of Σ onto $\bar{\Sigma}$ [resp. $\bar{\bar{\Sigma}}$], $\Sigma_b=\Sigma\cup\bar{\Sigma}\cup\bar{\bar{\Sigma}}$ and the free monoid Σ_b^* on Σ_b containing Σ^*.

$\forall w_1,w_2\in\Sigma_b^*$, $\forall z\in\Sigma$, the pair $(w_1w_2, w_1\bar{z}zw_2)$ denoted by $w_1w_2\to w_1\bar{z}zw_2$ is called a *left insertion of* $\bar{z}z$ and the pair (w_1w_2) denoted by $w_1\bar{z}zw_2\to w_1w_2$ is called a *left deletion of* $\bar{z}z$.

Similarly, the pair $(w_1w_2, w_1z\bar{\bar{z}}w_2)$ denoted by $w_1w_2\to w_1z\bar{\bar{z}}w_2$ is called a *right insertion of* $z\bar{\bar{z}}$ and the pair $(w_1z\bar{\bar{z}}w_2, w_1w_2)$ denoted by $w_1z\bar{\bar{z}}w_2\to w_1w_2$ is called a *right deletion of* $z\bar{\bar{z}}$.

If $\varrho\subset\Sigma^*\times\Sigma^*$ and $\varrho^{-1}=\{(u,v)\colon(v,u)\in\varrho\}$, $\forall w_1,w_2\in\Sigma_b^*$ and $\forall(u,u')\in\varrho\cup\varrho^{-1}\cup$

$\{(1,1)\}$, the pair $(w_1uw_2, w_1u'w_2)$ denoted by $w_1uw_2 \to w_1u'w_2$ is called an *elementary ϱ-transition.*

A pair $w \to w'$ with $w, w' \in \Sigma_b^*$ is called an *elementary ϱ-transformation* if $w \to w'$ is either an elementary ϱ-transition or a left or right insertion or a left or right deletion.

Definition 2.3. (i) If $n>0$ and, $\forall i \in \{0,\dots,n-1\}$, $w_i \to w_{i+1}$ is an elementary ϱ-transformation, the sequence $(s)=(w_0, w_1, \dots, w_n)$ denoted by $(s) \equiv w_0 \to w_1 \to \cdots \to w_n$ is called a *sequence of elementary ϱ-transformations from w_0 to w_n.*

$w_i \to w_{i+1}$ is then the *elementary ϱ-transformation of index i in* (s).

(ii) Any occurrence of a *letter z* of Σ_b is said to *keep its individuality in* (s) if

- $\forall i \in \{0,\dots,n\}$, $\exists u_i, v_i \in \Sigma_b^*$ such that $w_i = u_i z v_i$,
- $\forall i \in \{0,\dots,n-1\}$ either $u_{i+1}=u_i$ and $v_i \to v_{i+1}$ is an elementary ϱ-transformation or $v_{i+1}=v_i$ and $u_i \to u_{i+1}$ is an elementary ϱ-transformation.

The sequences $(s') \equiv u_0 \to u_1 \to \cdots \to u_n$ and $(s'') \equiv v_0 \to v_1 + \cdots + v_n$ of elementary ϱ-transformations are then called respectively the *z-left sequence* and the *z-right sequence of* (s).

(iii) Let $(s) \equiv w_0 \to w_1 \to \cdots \to w_n$ be a sequence of elementary ϱ-transformations.

If $I \equiv w_i \to w_{i+1}$ is an insertion of $\bar{z}z$ (resp. $z\bar{\bar{z}}$) in (s) and if $D \equiv w_j \to w_{j+1}$ is a deletion of $\bar{z}z$ (resp. $z\bar{\bar{z}}$) in (s) with $z \in \Sigma$ and $i<j$, then the *insertion I and* the *deletion D* are said to be *dual in* (s) when the subsequence $(s_{i+1}^j) \equiv w_{i+1} \to w_{i+2} \to \cdots \to w_j$ is a maximal subsequence of (s) in which $\bar{z}$ (resp. $\bar{\bar{z}}$) keeps its individuality.

(iv) Let $\mathrm{Il}(s)$ be the set of indices of the left insertions in (s), $\mathrm{Dl}(s)$ the set of indices of the left deletions in (s) and χ_l the partial mapping of $\mathrm{Il}(s)$ into $\mathrm{Dl}(s)$ such that, if i is the index of a left insertion I in (s) and if I has a dual deletion D, then $\chi_\mathrm{l}(i)$ is the index of D in (s), else χ_l is not definite for i.

We define similarly the partial mapping χ_r of $\mathrm{Ir}(s)$ into $\mathrm{Dr}(s)$.

A sequence (s) of elementary ϱ-transformations is called a *Malcev's sequence* if

(λ) χ_l is a bijection of $\mathrm{Il}(s)$ onto $\mathrm{Dl}(s)$ such that if $i<j<\chi_\mathrm{l}(i)$ with $i,j \in \mathrm{Il}(s)$, then $i<j<\chi_\mathrm{l}(j)<\chi_\mathrm{l}(i)$;

(μ) χ_r is a bijection of $\mathrm{Ir}(s)$ onto $\mathrm{Dr}(s)$ such that if $i<j<\chi_\mathrm{r}(i)$ with $i,j \in \mathrm{Ir}(s)$, then $i<j<\chi_\mathrm{r}(j)<\chi_\mathrm{r}(i)$.

The subsequence (sl) [resp. (sr)] of all left [resp. right] insertions and deletions in (s) is then a word of Dyck and the subsequence of all insertions and deletions in (s) is then a shuffle product of (sl) and (sr) (see [12] and [4]).

(v) Let $(s) \equiv w_0 \to w_1 \to \cdots \to w_n$ be a Malcev's sequence of elementary ϱ-transformations.

Any *left* [resp. *right*] *insertion* $I \equiv w_i \to w_{i+1}$ of $\bar{z}z$ (resp. $z\bar{\bar{z}}$) with $z \in \Sigma$ is said to be *proper* if, $D \equiv w_j \to w_{j+1}$ being the dual deletion of I in (s), all the words of the $\bar{z}$-left (resp. $\bar{\bar{z}}$-right) sequence of $(s_{i+1}^j) \to w_{i+1} \to w_{i+2} \to \cdots \to w_j$ are equal.

Any *Malcev's sequence* of elementary ϱ-transformations is said to be *proper* if all these insertions are proper.

Remark. The notion of proper insertion has been introduced by Malcev [8,9] and the following theorem is equivalent to his necessary and sufficient condition of embeddability of a semigroup in a group (see also [10, pp. 7–10; 1, pp. 31–34; 2, pp. 309–315]).

Theorem 2.4 (A.I. Malcev). *If Σ^* is the free monoid on the alphabet Σ and if $\varrho \subset \Sigma^* \times \Sigma^*$, a pair $(w, w') \in \Sigma^* \times \Sigma^*$ belongs to $m(\varrho)$ if and only if there exists a proper Malcev's sequence of elementary ϱ-transformations from w to w'.*

Lemma 2.5 (The three relators lemma). *Let $u, u', v, v', w_1, w_1', w_2$ and w_2' be words in Σ^*. Let R_0 be the relator $(uv, u'v')$ and define the relators R_1, R_2 and R_3 as in Table 1.*

Then in all cases, $R_3 \in m(\{R_0, R_1, R_2\})$, $R_2 \in m(\{R_0, R_1, R_3\})$, $R_1 \in m(\{R_0, R_2, R_3\})$ and $R_0 \in m(\{R_1, R_2, R_3\})$.

Table 1

Case	R_1	R_2	R_3
1	$(uw_1v, u'w_1'v')$	$(uw_2v, u'w_2'v')$	$(uw_1w_2v, u'w_1'w_2'v')$
2	$(uw_1v, u'w_1'v')$	$(uw_2v', u'w_2'v)$	$(uw_1w_2v', u'w_1'w_2'v)$
3	$(uw_1v', u'w_1'v)$	$(uw_2v, u'w_2'v')$	$(uw_1w_2'v', u'w_1'w_2v)$
4	$(uw_1v', u'w_1'v)$	$(uw_2v', u'w_2'v)$	$(uw_1w_2'v, u'w_1'w_2v')$

Proof. $\forall r \geq 0$, $\forall z_1, \ldots, z_r \in \Sigma$, $\forall \lambda, \mu \in \Sigma_b^*$, for $w = z_1 z_2 \ldots z_r$, let $\bar{w} = \bar{z}_r \bar{z}_{r-1} \ldots \bar{z}_1$ and $\bar{\bar{w}} = \bar{\bar{z}}_r \bar{\bar{z}}_{r-1} \ldots \bar{\bar{z}}_1$.

Let $\lambda\mu \xrightarrow{+} \lambda\bar{w}w\mu$ (resp. $\lambda\mu \xrightarrow{+} \lambda w\bar{\bar{w}}\mu$) be the sequence

$$\lambda\mu \to \lambda\bar{z}_r z_r \mu \to \lambda\bar{z}_r\bar{z}_{r-1}z_{r-1}z_r\mu \to \cdots \to \lambda\bar{z}_r\bar{z}_{r-1}\ldots\bar{z}_1 z_1 \ldots z_{r-1}z_r\mu = \lambda\bar{w}w\mu$$

(resp. $\lambda\mu \to \lambda z_1\bar{\bar{z}}_1\mu \to \lambda z_1 z_2 \bar{\bar{z}}_2 \bar{\bar{z}}_1 \mu \to \cdots \to \lambda z_1 \cdots z_r \bar{\bar{z}}_r \ldots \bar{\bar{z}}_1 \mu = \lambda w\bar{\bar{w}}\mu$) of left (resp. right) insertions and $\lambda\bar{w}w\mu \xrightarrow{+} \lambda\mu$ (resp. $\lambda w\bar{\bar{w}}\mu \xrightarrow{+} \lambda\mu$) its inverse sequence.

Case 1. (i) $R_3 \in m(\{R_0, R_1, R_2\})$ since

$$\begin{aligned} &uw_1w_2v \xrightarrow{+} uw_1\bar{u}uw_2v \to uw_1\bar{u}u'w_2'v' \xrightarrow{+} uw_1\bar{u}u'v'\bar{\bar{v}}'w_2'v' \to \cdots \\ &\cdots \to uw_1\bar{u}uv\bar{\bar{v}}'w_2'v' \xrightarrow{+} uw_1v\bar{\bar{v}}'w_2'v' \to u'w_1'v'\bar{\bar{v}}'w_2'v' \xrightarrow{+} u'w_1'w_2'v' \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_0, R_1, R_2\}$-transformations.

(ii) $R_2 \in m(\{R_0, R_1, R_2\})$ since

$$\begin{aligned} &uw_2v \xrightarrow{+} u\bar{w}_1w_1w_2v \xrightarrow{+} u\bar{w}_1\bar{u}uw_1w_2v \to u\bar{w}_1\bar{u}u'w_1'w_2'v' \to \cdots \\ &\cdots \xrightarrow{+} u\bar{w}_1\bar{u}u'w_1'v'\bar{\bar{v}}'w_2'v' \to u\bar{w}_1\bar{u}uw_1v\bar{\bar{v}}'w_2'v' \xrightarrow{+} u\bar{w}_1w_1v\bar{\bar{v}}'w_2'v' \to \cdots \\ &\cdots \xrightarrow{+} uv\bar{\bar{v}}'w_2'v' \to u'v'\bar{\bar{v}}'w_2'v' \xrightarrow{+} u'w_2'v' \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_0, R_1, R_3\}$-transformations.

(iii) Similarly $R_1 \in m(\{R_0, R_2, R_3\})$.

(iv) $R_0 \in m(\{R_1, R_2, R_3\})$ since

$$\begin{aligned} uv &\xrightarrow{+} u\bar{w}_1 w_1 v \xrightarrow{+} u\bar{w}_1 \bar{u} u w_1 v \to u\bar{w}_1 \bar{u} u' w_1' v' \xrightarrow{+} u\bar{w}_1 \bar{u} u' w_1' w_2' \bar{\bar{w}}_2' v' \to \cdots \\ &\cdots \xrightarrow{+} u\bar{w}_1 \bar{u} u' w_1' w_2' v' \bar{\bar{v}}' \bar{\bar{w}}_2' v' \to u\bar{w}_1 \bar{u} u w_1 w_2 v \bar{\bar{v}}' \bar{\bar{w}}_2' v \xrightarrow{+} u\bar{w}_1 w_1 w_2 v \bar{\bar{v}}' \bar{\bar{w}}_2' v' \to \cdots \\ &\cdots \xrightarrow{+} u w_2 v \bar{\bar{v}}' \bar{\bar{w}}_2' v' \to u' w_2' v' \bar{\bar{v}}' \bar{\bar{w}}_2' v' \xrightarrow{+} u' w_2' \bar{\bar{w}}_2' v' \xrightarrow{+} u' v' \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_1, R_2, R_3\}$-transformations.

We prove here that $R_3 \in m\ (\{R_0, R_1, R_2\})$ in Cases 2, 3 and 4 because this result is used in Lemma 2.7. The omitted proofs of the other subcases are very similar to the proofs for Case 1.

Case 2. $R_3 \in m(\{R_0, R_1, R_2\})$ since

$$\begin{aligned} u w_1 w_2 v' &\xrightarrow{+} u w_1 \bar{u} u w_2 v' \to u w_1 \bar{u} u' w_2' v \xrightarrow{+} u w_1 \bar{u} u' v' \bar{\bar{v}}' w_2' v \to \cdots \\ &\cdots \to u w_1 \bar{u} u v \bar{\bar{v}}' w_2' v \xrightarrow{+} u w_1 v \bar{\bar{v}}' w_2' v \to u' w_1' v' \bar{\bar{v}}' w_2' v \xrightarrow{+} u' w_1' w_2' v \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_0, R_1, R_2\}$-transformations.

Case 3. $R_3 \in m(\{R_0, R_1, R_2\})$ since

$$\begin{aligned} u w_1 w_2' v' &\xrightarrow{+} u w_1 \bar{u}' u' w_2' v' \to u w_1 \bar{u}' u w_2 v \xrightarrow{+} u w_1 \bar{u}' u v \bar{\bar{v}} w_2 v \to \cdots \\ &\cdots \to u w_1 \bar{u}' u' v' \bar{\bar{v}} w_2 v \xrightarrow{+} u w_1 v' \bar{\bar{v}} w_2 v \to u' w_1' v \bar{\bar{v}} w_2 v \xrightarrow{+} u' w_1' w_2 v \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_0, R_1, R_2\}$-transformations.

Case 4. $R_3 \in m(\{R_0, R_1, R_2\})$ since

$$\begin{aligned} u w_1 w_2' v &\xrightarrow{+} u w_1 \bar{u}' u' w_2' v \to u w_1 \bar{u}' u w_2 v' \xrightarrow{+} u w_1 \bar{u}' u v \bar{\bar{v}} w_2 v' \to \cdots \\ &\cdots \to u w_1 \bar{u}' v' u' \bar{\bar{v}} w_2 v' \xrightarrow{+} u w_1 v' \bar{\bar{v}} w_2 v' \to u' w_1' v \bar{\bar{v}} w_2 v' \xrightarrow{+} u' w_1' w_2 v' \end{aligned}$$

is a proper Malcev's sequence of elementary $\{R_0, R_1, R_2\}$-transformations.

Definition 2.6. If $R = (u, u')$ is a relator of C^*, then the length of the word $\alpha(u) = \alpha(u')$ in A^* is called the *length of the relator* R and is denoted by $|R|$.

$\forall r > 0$, let ϱ_r be the set of all relators R of C^* such that $|R| < r$.

Any *relator* R of C^* is said to be *m-deductible* if $R \in m(\varrho_r)$ with $r = |R|$. Otherwise R is said to be *m-indeductible.*

Let $<$ be any lexicographical order in the free monoid Σ^* and let τ be the set of all m-indeductible relators (u, u') of C^* such that $u < u'$.

Lemma 2.7 (The lemma of m-deductibility). *Every relator produced by a unitary circuit of $\mathscr{L}(C)$ which passes more than twice by some vertex of $\mathscr{L}(C)$ is m-deductible.*

Proof. Let $R = (w, w')$ be a relator of C^* produced by a unitary circuit $\sigma = ((1, d_1)_{(z_1, \omega_1)}, (d_1, d_2)_{(z_2, \omega_2)}, \ldots, (d_{n-1}, 1)_{(z_n, \omega_n)})$ which passes more than twice by the vertex d of $\mathscr{L}(C)$ and let $r = |R|$.

If $d = 1$, then R is a product of relators in ϱ_r and the result is trivial.

If $d \neq 1$, $\exists i, j, k \in \{1, \ldots, n-1\}$ such that $d_i = d_j = d_k = d$ with $i < j < k$. Let

$$\tau_1 = ((1, d_1)_{(z_1, \omega_1)}, \ldots, (d_{i-1}, d_i)_{(z_i, \omega_i)}),$$
$$\sigma_1 = ((d_i, d_{i+1})_{(z_{i+1}, \omega_{i+1})}, \ldots, (d_{j-1}, d_j)_{(z_j, \omega_j)}),$$
$$\sigma_2 = ((d_j, d_{j+1})_{(z_{j+1}, \omega_{j+1})}, \ldots, (d_{k-1}, d_k)_{(z_k, \omega_k)}),$$
$$\tau_2 = ((d_k, d_{k+1})_{(z_{k+1}, \omega_{k+1})}, \ldots, (d_{n-1}, 1)_{(z_n, \omega_n)})$$

be the paths such that $\sigma = \tau_1\sigma_1\sigma_2\tau_2$.

Let (u, u'), (w_1, w_1'), (w_2, w_2') and (v, v') be the patterns respectively produced by τ_1, σ_1, σ_2 and τ_2 such that

- $\alpha(u) = \alpha(u')d$;
- $\alpha(w_1')d = d\alpha(w_1)$ (resp. $\alpha(w_1') = d\alpha(w_1)d$) if the length $j-i$ of the circuit σ_1 is even (resp. odd);
- $\alpha(w_2')d = d\alpha(w_2)$ (resp. $\alpha(w_2') = d\alpha(w_2)d$) if the length $k-j$ of the circuit σ_2 is even (resp. odd);
- $\alpha(v') = d\alpha(v)$.

The relators R_0, R_1, R_2 and R respectively produced by the unitary circuits $\tau_1\tau_2$, $\tau_1\sigma_1\tau_2$, $\tau_1\sigma_2\tau_2$ and $\tau_1\sigma_1\sigma_2\tau_2 = \sigma$ are then

- $R_0 = (uv, u'v')$;
- $R_1 = (uw_1v, u'w_1'v')$ (resp. $R_1 = (uw_1v', u'w_1'v)$) if the length of σ_1 is even (resp. odd);
- $R_2 = (uw_2v, u'w_2'v')$ (resp. $R_2 = (uw_2v', u'w_2'v)$) if the length of σ_2 is even (resp. odd);
- $R = (uw_1w_2v, u'w_1'w_2'v')$ (resp. $R = (uw_1w_2'v, u'w_1'w_2v')$) if the lengths of σ_1 and σ_2 are even (resp. odd);
- $R = (uw_1w_2v', u'w_1'w_2'v)$ (resp. $R = (uw_1w_2'v', u'w_1'w_2v)$) if the length of σ_1 is even (resp. odd) and that of σ_2 is odd (resp. even).

By Lemma 2.5, $R \in m(\{R_0, R_1, R_2\})$ and, since $|R_i| < |R|$ for $i \in \{0, 1, 2\}$, $R \in m(\varrho_r)$, that is, R is m-deductible.

Theorem 2.8. *Every finitely generated submonoid of a free monoid has a finite Malcev's presentation and such a finite presentation can be effectively found.*

Proof. Let M be a finitely generated submonoid of the free monoid A^* on the alphabet A.

(i) The smallest generating set $C = M^+ \setminus (M^+)^2$ of M is then finite.

Since, $\forall c \in C$, $\mathrm{Fb}(c)$ is finite and the set of labeled Σ-pairs $(d, d')_{(z, \omega)}$ with $\alpha(z) = c$ also, the graph $\mathscr{L}(C)$ of relators of C^* is finite.

It follows that the set of unitary circuits of $\mathscr{L}(C)$ which pass at most twice by some vertex of $\mathscr{L}(C)$ is also finite and, by Lemma 2.7, the set τ of m-indeductible relators of C^* also.

(ii) By definition $\tau \subset \mathrm{Ker}\,\alpha$. Since the free monoid A^* and hence its submonoid

M are embeddable in the free group on the alphabet A, $\operatorname{Ker}\alpha$ is a Malcev's congruence. Consequently $m(\tau)\subset\operatorname{Ker}\alpha$.

$\varrho_1=\{(1,1)\}\subset m(\tau)$. If $\varrho_r\subset m(\tau)$ then, for every relator R of C^* of length $|R|=r$, either R is m-deductible showing that $R\in m(\varrho_r)\subset m(\tau)$ or R is m-indeductible showing that $R\in\tau\cup\tau^{-1}\subset m(\tau)$. Thus $\varrho_{r+1}\subset m(\tau)$.

It follows that $\operatorname{Ker}\alpha=\bigcup_{r>0}\varrho_r\subset m(\tau)$ and, finally, that $\operatorname{Ker}\alpha=m(\tau)$. Thus (Σ,τ) is a finite Malcev's presentation of C^*.

(iii) The finite graph $\mathscr{L}(C)$ can be found effectively and, consequently, the set τ of m-indeductible relators of C^* also.

Example 2.9. If C^* is the submonoid of A^* given in Example 1.3, the relator (xzz, yyx) produced by the unitary circuit

$$\sigma=((1,b)_{(y,x)},(b,a)_{(z,1)},(a,b)_{(y,1)},(b,1)_{(z,x)})$$

is m-deductible since $xzz\to yxz\to yyx$ is a sequence of elementary $\{(xz,yx)\}$-transitions. By Theorem 2.8, $\tau=\{(xz,yx),(xux,yz)\}$ and (Σ,τ) is a Malcev's presentation of C^*.

Moreover, this monoid C^* has neither a finite presentation nor a finite cancellative presentation [12].

Remark 2.10. We can compare the proof of Theorem 2.8 with the simpler proof given by Karhumäki [5] (see also [3]) for the following theorem: "Every rational language L of a free monoid Σ^* on a finite alphabet Σ contains a finite subset F such that, for all homomorphisms α and β of Σ^* in some free monoid, $\alpha/F=\beta/F$ implies $\alpha/L=\beta/L$" by exchanging the graph $\mathscr{L}(C)$ with one finite automata and the three relators lemma with a three equations lemma – which is a special case of the above lemma.

Remark 2.11. A subset S of $\Sigma^*\times\Sigma^*$ is again called a system of equations on the alphabet Σ and the letters of Σ are called the variables of S.

A morphism α of Σ^* in some free monoid is called a solution of the system S' if, $\forall(u,v)\in S$, $\alpha(u)=\alpha(v)$. (See [7].)

Two systems S and T are said to be equivalent if S and T have the same solutions.

A system S is said to be entire if there exists a solution α of S such that $S=\operatorname{Ker}\alpha$.

Since $S=\alpha^{-1}\circ\alpha$, S is then a rational subset of $\Sigma^*\times\Sigma^*$. (See [4, p. 236–248].)

We can deduce from Theorem 2.8 that the set τ of m-indeductible relators of C^* is equivalent to the entire system $S=\operatorname{Ker}\alpha$. (See [14].)

Acknowledgment

I wish to express my gratitude to the anonymous referee whose advice has greatly helped to enhance the presentation of this paper.

References

[1] S.I. Adjan, Defining relations and algorithmic problems for groups and semigroups, Proc. Steklov Inst. Math. 85 (1967) 1-152.

[2] A.H. Clifford and G.B. Preston, The Algebraic Theory of Semigroups (Amer. Math. Soc., Providence, RI, 1967).

[3] K. Culik, II and A. Salomaa, On the decidability of homomorphism equivalence for languages, J. Comput. System Sci. 17 (1978) 163-175.

[4] S. Eilenberg, Automata, Languages and Machines, Vol. A (Academic Press, New York, 1974).

[5] J. Karhumaki, The Ehrenfeucht conjecture: a compactness claim for finitely generated free monoids, Theoret. Comput. Sci. 29 (1984) 285-308.

[6] G. Lallement, Semigroups and Combinatorial Applications (Wiley, New York, 1979).

[7] A. Lentin, Equations dans le Monoïde Libre (Gauthier-Villars, Paris, 1972).

[8] A.I. Malcev, On the immersion of associative systems in groups, Mat. Sb. (N.S.) 6 (1939) 331-336 (in Russian).

[9] A.I. Malcev, On the immersion of associative systems in groups II, Mat. Sb. (N.S.) 8 (1940) 251-264 (in Russian).

[10] P.S. Novikov, On the algorithmic unsolvability of the word problem in group theory, Amer. Math. Soc. Transl. (2) 9 (1958) 1-122.

[11] J.C. Spehner, Quelques constructions et algorithmes relatifs aux sous-monoides d'un monoide libre, Semigroup Forum 9 (1975) 334-353.

[12] J.C. Spehner, Présentations et présentations simplifiables d'un monoide simplifiable, Semigroup Forum 14 (1977) 295-329.

[13] J.C. Spehner, On external conjugation of submonoids of a free monoid, in: G. Pollák, ed., Algebraic Theory of Semigroups, Colloq. Mat. Soc. János Bolyai 20 (North-Holland, Amsterdam, 1979) 545-576.

[14] J.C. Spehner, Systèmes entiers d'équations sur un alphabet fini et Conjecture d'Ehrenfeucht, Theoret. Comput. Sci. 39 (1985) 171-188.